960603-5

[POST COPY]

PROCESS FOR ENTRY OF A CONFIDENTIAL PIECE OF INFORMATION AND ASSOCIATED TERMINAL

The present invention relates to a process for entry of a confidential piece of information furnished by a user at a terminal, this information comprising several signs which belong to a first series of signs.

It is known that means for electronic payment using a card associated with a terminal are becoming widespread, and that these include ticket dispensers and in-store means of payment.

In order to identify a card holder or an operator, this person is often required to input a confidential piece of information, usually called a code, by means of a keyboard associated with the terminal. The conditions under which this code must be input by means of the keyboard do not generally permit the keyboard to be satisfactorily hidden, so that it can be observed by a third party during the entry of the confidential information. An ill-intentioned person can then use this information to fraudulent ends.

Certain systems include keyboards whose signs are disposed in positions that vary from one keyboard to another so that it is not possible for a third party who does not know the disposition of the signs on a keyboard in the course of being used to guess

the confidential information simply by observing the position of the keys the user strikes. This, however, has the drawbacks of substantially complicating the embodiment of the keyboard and of engendering errors in the inputting of the confidential information when users who are used to a certain disposition of the signs do not pay attention to the fact that the keyboard in question does not have the usual disposition. In addition, an experienced defrauder can analyze the redistribution of the signs on a specific keyboard either before or after the entry of the confidential information by the user and memorize the position of the keys struck in order to eventually deduce the confidential information.

One object of the present invention is to propose a process for protecting a confidential piece of information comprising several signs which belong to a first series of signs during the entry of this information, even when this operation may be observed by a third party.

With a view to the achievement of this object, the process according to the invention consists of defining a second series of signs; of displaying the first and second series of signs on a display means so that each sign in the first series will be disposed opposite a sign in the second, and of using the signs in the second series of signs, opposite which the signs in the first series composing the confidential information are disposed, for

the user's designation of the confidential information.

Thus, the user does not directly designate the signs which compose the confidential information, but rather the signs -- those in the second series -- which are correlated with these signs in accordance with a correlation site that does not appear explicitly on the display means. Consequently, merely observation of the display means by a third party does not permit him or her to deduce the confidential signs that are entered.

In a first variant of the process according to the invention, one makes use of a keyboard which is distinct from the display means and which comprises a plurality of keys, identifies each of the keys on the keyboard by assigning it a sign that belongs to the second series of signs, and displays the first and second series of signs on the display means in a random mutual distribution that is known to the terminal; the user designates the signs in the first series which compose the confidential information by depressing each key on the keyboard whose sign corresponds to the sign in the second series that is located opposite one of the signs belonging to the first series which constitute the confidential information.

Thus, when a user enters a confidential piece of information, the keys on the keyboard that he or she strikes do not include the signs of his or her code, but corresponding signs

in accordance with a correspondence that is given to the user by means of simultaneous display of the two series of signs. Given that this correspondence varies with each entry of the confidential information as a function of the relative positioning of the series of signs, the only possible recognition of the keys struck on the keyboard during an entry is useless to a defrauder.

According to one advantageous version of this aspect of the invention, at least one of the series of signs disappears as soon as a key is struck. Thus, it is not possible for a defrauder to first see the key that is struck and then learn the sign that corresponds to the first series by observing the series that are displayed.

With the aid of the versions described previously, the user can henceforth enter a confidential piece of information without divulging the slightest indication to a third party, who can only see the keyboard or the screen.

According to a second variant of the process according to the invention, a solution is brought to bear on the problem of a third party who can observe the screen and the keyboard at the same time; in order to do this, at least one reference sign known to the terminal and to the user is secretly defined from among the signs in the second series, and then the signs in the first

series of signs are displayed opposite the signs in the second series in such a way that each time, one of the signs which compose this confidential information is disposed opposite the reference sign.

In an advantageous version of this aspect of the invention, during the entire entry operation, the set of signs in the first series is displayed in arbitrary order; the set of signs is shifted in relation to the signs in the second series so that at least one confidential sign composing the confidential information is disposed in front of the reference sign; and the entry is validated when the user gives the terminal a validation order indicated that this confidential sign has been place in front of the reference sign.

According to yet another version of the invention in which the terminal includes a keyboard with a plurality of keys, each of the keys on the keyboard is identified by being assigned a sign that belongs to the first series of signs, and for each key that is depressed, the sign in the first series assigned to this key is displayed opposite a sign in the second series; the terminal is arranged in order to effect a comparison between the sign in the first series that has thus been placed by the user in front of the reference sign and at least one of the signs of the confidential information.

The invention also relates to a terminal including a display means and means for entering a confidential piece of information furnished by a user, this information comprising several signs belonging to a first series of signs; the terminal is arranged in order to display the first and a second series of signs on the display means so that each sign in the first series will be disposed opposite a sign in the second series, and it comprises, on one hand, means for using the signs in the second series located opposite the signs that constitute the confidential information to allow the user to designate the signs in the first series that compose the confidential information, and on the other hand, means for validating the entries.

Other characteristics and advantages of the invention will become apparent upon a reading of the following description of different versions of the invention in connection with the appended figures, in which:

- Fig. 1 schematically illustrates part of a terminal using a first variant of the process according to the invention,

- Fig. 2 is a schematic representation of the display screen at a later stage than in Fig. 1, relating to a variant of implementation of the process according to the invention,

- Fig. 3 is a schematic illustration of the screen of a

terminal relating to another version of the process according to the invention,

- Fig. 4 is a later illustration of the screen of the terminal than in Fig. 3, which relates to the version of the process in Fig. 3,

- Fig. 5 is another illustration of the process according to Fig. 3, comprising a second series of signs which are constituted by arrows, and

- Fig. 6 schematically illustrates part of a terminal using a second variant of the process according to the invention.

In reference to Fig. 1, a first variant of implementation of the process according to the invention is intended to make it possible to protect a confidential piece of information, for example the code of a bank card, during its entry on the keyboard of a terminal. Fig. 1 represents only the keyboard of the terminal, designated generally as 1, and the display screen of the terminal, designated generally as 2. In a manner known per se, the confidential information is composed of signs which belong to a series of signs, for example digits in the example illustrated. Following the description, it will be assumed that the confidential information is composed of four signs and that in the examples illustrated, these four signs are the digits

According to this variant of the invention, a second series of signs is represented on the keys 5 of the keyboard 1 of the terminal, and on one hand a first series of signs, disposed here in a line 3 on the display screen, and on the other hand the second series of signs, disposed here in a line 4 on the display screen above the first series of signs in the line 3, are displayed on the terminal; the first and second series of signs are displayed according to a random relative position, which means that the correspondence between the signs in the first series and the signs in the second series can vary each time a card is inserted into the terminal. Thus, the keys on the keyboard which must be struck vary with each new display of the two series of signs so that a third party who observes only the keys struck by the user will not be able to reuse the information thus obtained during a subsequent entry.

According to a first version of the invention, it is assumed that the first and second series of signs continue to be displayed in the same relative position while the user enters the different signs on the keyboard. In the case envisioned, the user will then successively strike the keys on the keyboard comprising θ, then ⊕, then π, and finally ♥. In order to facilitate the user's entry of the confidential information, the display screen 2 usually and preferably comprises a line 6 of

marks which indicate the number of signs already entered, thus allowing the user to know what position in the confidential information he has reached. In the example illustrated, the signs in the line 6 begin as dots, and are progressively replaced with asterisks each time the user enters a sign.

It will be noted that in this version of the process of the invention a defrauder who observes only the keyboard will not in any way understand the confidential information since he does not know the correspondence between the signs struck on the keyboard and the digits which compose the code. If, however, he is also capable of seeing the screen, he will be able to memorize the correspondence between the two series of signs, or more simply, to look at this correspondence each time he sees the user strike one of the keys on the keyboard. In fact, reading the correspondence involves a relatively sustained effort on the part of the user who tends to verify that he is not making a mistake with the signs in the second series and therefore proceeds more slowly than usual. In this case, it will therefore be possible for a defrauder who has seen the user strike the key 8 to then look at the screen and discover that 8 corresponds to the digit 4, and thus to successively execute a decoding of the signs struck by the user.

In order to avoid such a maneuver on the part of the defrauder, another version of the invention envisions preferably

changing the relative position of the first and the second series of signs after each sign of the confidential information is entered. Thus, even when a third party is capable of observing not only the keyboard but also the display of the series of signs, the considerable frequency of change in the correspondence between the signs in the first series and in the second series increases the difficulty of memorizing this correspondence simultaneously with the position of the key struck by the user. Fig. 2 illustrates the display which the user sees on the screen as soon as he strikes the key 0. According to the version illustrated, the second series of signs is left in the same position but the first series of signs is displayed in a new disposition of the digits, while in the line of marks 6 the first dot has been replaced by a asterisk. According to this version of the invention, after having begun as before by striking the key 0, this time the user will strike the key 4 which corresponds to the second digit of his or her code, in this case 7. It will be noted, therefore, that it is not possible for a defrauder who has waited to see the key struck by the user to determine the corresponding sign in the first series. In fact, the defrauder who has waited and has seen the user strike the key 0 and who then looks at the display screen will read that the digit corresponding to 0 is the digit 3 and will thus make an error in guessing the first digit of the confidential information. In order to be able to obtain the confidential information, the defrauder would therefore have to be able to successively

memorize the correspondences between the first and the second series of signs before the user has struck a sign, which considerably reduces the risk that a defrauder would be able to memorize the set of signs of the confidential information.

In the example illustrated in Figs. 1 and 2, the two series of signs are displayed on the screen, but only the signs in the first series have a variable position. It will be noted that it is of course also possible to vary the position of the signs in the second series, or even to vary the position of the signs in the second series while holding the signs in the first series in a fixed position.

Figs. 3 through 5 illustrate another version of the process according to the invention. In this version, the signs in the second series are now disposed below the signs in the first series, and they are permanently disposed on the housing of the terminal below the display screen. This disposition does not characterize this version of the process of the invention, and it would be possible to adopt the same disposition for the signs as in Figs. 1 and 2. What does characterize this version of the process of the invention is the fact that the second series of signs now comprises a distinct number of distinct signs that is lower than in the first series of signs, so that in order to have a correspondence between each of the signs in the first series and the signs in the second series, it is necessary to assign the

same sign in the second series to several signs in the first series. In the example illustrated in Figs. 3 and 4, the first series of signs comprises, as before, ten digits from zero to 9, and the second series of signs now comprises only five distinct signs which are ⊙, θ, ☼, ♥, ☎. In order for a sign in the second series to correspond to each sign in the first series, certain signs in the second series are represented with a brace in order to show the signs in the first series to which they are assigned. Thus the ⊙ is assigned to two digits as are the θ and the ♥, while the ☼ is assigned to three digits and the ☎ is assigned to a single digit.

When a card is inserted, the signs in the first series are displayed randomly so that one sign in the second series corresponds to each sign in the first series. In this regard, it will be noted that the position of the signs in the first series can be totally random, which means that the signs in the first series are disposed randomly not only relative to the signs in the second series but also relative to one another, or in a pseudo-random fashion, which means that while being disposed randomly relative to the signs in the second series, the digits in the first series are disposed in sequence relative to one another. This is the case in the example illustrated in Fig. 3, in which the digits are arranged relative to one another in a loop sequence, and their random position relative to the signs in the second series is determined by a random shift in the

sequence. In Fig. 3 in particular, the zero corresponds to the second box, with a ✡, in the second series.

Assuming that the position of the signs in the first series remains constant during the entire entry of the confidential information, a user who has the code 4723 will then enter, in the case of Fig. 3, the signs θ, ✡, ♥ and ❁ successively. Contrary to the version which has been described in relation to Fig. 1, a defrauder who simultaneously observes the keyboard and the screen will not be able to deduce the confidential information entered by the user with certainty. In effect, when a defrauder sees the user enter the first sign θ, he can not know if this sign corresponds to digit 1 or to digit 4. Likewise, when the user enters the sign ✡, an observer cannot know if this ✡ corresponds to the digit 0, the digit 5, or to the digit 7. In the same way, the sign ♥ may correspond to either the digit 0 or the digit 8. Only the sign ❁ corresponds solely to the digit 6. In this case the same sequence of signs in the second series would have been entered by the user whether the code were 1529 or 4089.

Assuming that an observer has succeeded in memorizing the entire correspondence between the signs in the first and second series and the order in which the keys have been struck by the user, and assuming that he would want to reuse this information during a subsequent entry, he will find himself confronted with a new table of correspondence as illustrated, for example, in Fig.

4. In this figure, a new [illegible] has been executed between the series of digits forming the first series of signs and the second series of signs. It so happens that the choice between the 1 and the 4 which could have been [illegible] an observer during the preceding entry, is now illustrated by a [illegible] and a [illegible], which means that there is one chance in [illegible] that the defrauder will make a mistake in the entry of the first sign constituting the confidential information. However, a defrauder will again have a doubt concerning the second sign to be entered, since the digits 0, 5 and 7 which corresponded to the sign [illegible] in Fig. 3 are represented in Fig. 4 by the signs [illegible], [illegible] or [illegible]. Note that the probability of an observer [illegible] able to reenter the confidential information [illegible] extremely low. This risk is further minimized if, as previously, it has been envisioned that the correspondence between the first series of signs and the second series of signs will change each time a sign has been entered.

The variant in Fig. [illegible] is distinguished from that in Fig. 3 in that the sophisticated signs constituted by the signs in the second series have been replaced here by simpler signs which are made of a single elementary sign, namely an isosceles triangle. The second series of signs comprises five signs, each of which is distinguished by a specific number of triangles or by a specific orientation of them. Thus, all three of the digits 2 through 4 in the first series of signs are denoted by the same sign,

This Sheet Has Been Replaced

which in Fig. 5 is constituted by two juxtaposed triangles 6 oriented toward the right. A brace 7 defines this correspondence. The digits 0 and 1 are designated by a single triangle 6 with the same orientation as for the digits 2 through 4. A second series of this type, made of a single simple sign, is advantageous in that the use immediately memorizes the set of signs used. In addition, the digits in the first series of signs (for example 2 through 4) that are designated by the same sign in the second series are juxtaposed, so that a single sign (here the two triangles 6) designates them both simultaneously, which further facilitates the user's task.

Fig. 6 illustrates another variant of implementation of the process in which it is assumed that, in addition to the digits 4723, the user's confidential code includes two secret reference signs 3 and 9 among the signs in the second series, and that all these signs are known to the user and to the terminal at the time of the entry. These reference signs can, for example, be provided to the user by the authorizing institution, along with the confidential information, upon subscription to the service is requested.

In this Fig. 6 the two series are identical, and the signs which compose them here are the digits 0 through 9. The terminal displays the second series of signs 61, either in a permanent fashion, with the signs etched into the display means, or in a

random fashion. The display boxes have been arranged so as to display the signs in the first series, which are to be entered, opposite the signs in the second series. In the example of Fig. 6, the boxes 63 which correspond to the boxes placed opposite the reference signs 3 and 9 have been grayed in. Of course, since the display on the screen is non-specialized, there is no indication which might allow a defrauder to determine which of the displayed signs are the reference signs.

The keyboard 65 associated with these display means comprises keys identified by the signs 0 through 9 and it permits the user to enter these signs, which are then displayed in the boxes located opposite the signs in the second series as soon as the entries are made. The user will then enter unimportant signs into all the boxes other than these two, which here are referred to as 63. Conversely, he or she enters the first two digits, 4 and 7, of his or her confidential information into these boxes 63. This entry is complete when all the boxes are filled; the terminal then directs the user to again enter a series of signs opposite the series comprising the reference signs, so as to enter in the same way the two remaining digits of his or her confidential information, 2 and 3. For a third-party observer it is possible, with added memorization effort, to remember the complete combination that has been entered, but he or she has no way to determine which of the signs has any particular importance. In the case in which the signs in the second series

are displayed randomly from the start, entering this combination would avail him nothing.

A system for scrolling the signs in the first series, in a sequence that is displayed opposite the second series, may also be envisioned. For this purpose, means for shifting these signs have been provided. For example, two shift keys, respectively on the left and on the right, or even a single key, may be used to initiate cyclical scrolling of the signs in the first series.

Each time one of these keys is pressed, or after a given, very brief time lapse, the sequence is then shifted by one position in the chosen direction, and this is done cyclically so that there will always be a sign in the first series placed opposite a sign in the second. When the first sign of the confidential information is located opposite one of the reference signs, the user gives a validation order, for example using a validation key or a vocal command.

The signs of at least one of the two series are then displayed in a new random sequence before the entry of the next sign of the confidential information. Generally this is enough to indicate to the user that the preceding sign has been effectively captured by the system and that the system is waiting for the next entry.

The cycle repeats itself until all the confidential information has been entered. At the end of the operation, it is possible to simply display a message or erase the sequences of signs, which signals to the user that the entry has been completed. It is possible to envision the display of a character, for example the sign *, for each sign entered.

In the case presented in Fig. 6, the signs of the confidential information are entered in an ordered fashon, according to an arrangement (1...i...n). In order to confuse an observer, this information can be entered in a disordered fashion. To this end, the terminal displays a message directing the user to place his or her sign(s) that are in the i position opposite his or her reference sign(s). In this way, the entry order is shuffled, and it changes with each new entry.

In the case in which the confidential information is composed of digits, as in the example in Fig. 6, the terminal's message can also direct the user to place the digit, which results from a function of those digits of his or her confidential information that are in the i and j positions, opposite the reference signs. Of course, this function is modified with each entry.

Let it be supposed for now that the message comprises:

Secret box 1: enter the third digit of your code, plus 1.

Secret box 2: enter the first digit of your code, minus 1.

The user must then enter the digits 3 (digit 2 plus 1) and 3 (digit 4 minus 1) into the boxes 63 which correspond to the reference signs. A potential defrauder who gains knowledge of the message and who retains the digits that are entered does not know to which of the entered digits he must apply these functions in order to obtain the confidential information.

It is understood that the invention is not limited to the mode of embodiment described and variant embodiments may be achieved without departing from the scope of the invention. In particular, although the signs in the first series have been illustrated by digits, any signs may be envisioned; the signs used may even be different from one card to another, and the display of the signs in the first series would then be produced by the terminal as a function of a codification contained in the card.

It is also possible to envision identical signs for the first and the second series of signs. In this case it would be necessary that the series of signs be clearly indicated on the

display screen; otherwise the risk of errors in the entry may be too great.

CLAIMS



1. Process for entry of a confidential piece of information furnished by a user at a terminal, this information including a plurality of signs which belong to a first series of signs (3), characterized in that it comprises the following steps, which consist of:

- defining a second series of signs (4);
- displaying the first and second series of signs on display means so that each sign in the first series of signs will be disposed opposite a sign in the second series of signs; and
- using the signs in the second series of signs, opposite which the signs in the first series of signs composing said confidential information are disposed, for the user's designation of the confidential information.

2. Process according to claim 1, characterized in that it makes use of a keyboard (1) which is distinct from the display means and which includes a plurality of keys, and in that one proceeds to the following steps, which consist of:

- identifying each of the keys on a keyboard by assigning it a sign which belongs to the second

series of signs (4);

- displaying the first and second series of signs on the display means in a mutual random distribution that is known to the terminal; and

- designating the signs in the first series which compose said confidential information by depressing each key on the keyboard (1) whose sign corresponds to the sign in the second series (4) located opposite one of the signs in the first series (3) constituting said confidential information.

3. Process according to claim 2, characterized in that at least one of the series of signs (3,4) disappears as soon as a key on the keyboard (1) is struck.

4. Process according to claim 1, characterized in that it includes the following steps:

- secretly defining at least one reference sign, from among the signs in the second series (4), that is known to the terminal and to the user; and

- displaying the signs in the first series of

signs opposite the signs in the second series so that each time, one of the confidential signs which compose said confidential information will be disposed opposite said reference sign.

5. Process according to claim 4, characterized in that:

- during the entire entry operation, the set of signs in the first series (3) is displayed in arbitrary order;

- the set of signs (3) is shifted in relation to the signs in the second series (4) so that at least one confidential sign composing said confidential information is disposed in front of said reference sign; and

- the user gives the terminal a validation order when this confidential sign is disposed in front of the reference sign.

6. Process according to claim 4, characterized in that one makes use of a keyboard (1) with a plurality of keys, in which each of the keys is identified by being assigned a sign which belongs to the first series of signs (3), and in which the display of each of the signs in the first series (3) opposite the

* C L M S *

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

signs in the second series (4) is produced by depressing the key identified by this sign, the terminal being arranged in order to effect a comparison between the sign in the first series that has thus been placed by the user in front of the reference sign and at least one of the signs of the confidential information.

7. Process according to claim 6, characterized in that this confidential information includes several confidential signs arranged in a predetermined order (1...i...n), and that before the user displays the signs in the first series (3), the terminal gives him or her a message directing him or her to place the confidential sign that is in the i position opposite the reference sign.

8. Process according to claim 7, characterized in that the signs in the first series (3) which compose said confidential information are digits, and that the terminal directs the user to place the result of a function of the digit that is in the i position of said confidential information opposite the reference sign.

9. Process according to claim 1, characterized in that the second series of signs (4) includes a number of distinct signs that is less than the number of signs in the first series (3).

10. Process according to claim 1, characterized in that the

signs in the second series (4) are different from those in the first series (3).

11. Terminal including a display means and means to enter a confidential piece of information furnished by a user, said information including a plurality of signs which belong to a first set of signs (3), said terminal being characterized in that it is arranged in order to display said first and a second series of signs (4) in such a way that each sign in the first series (3) is disposed opposite a sign in the second series (4), and it comprises:

- means for using the signs in the second series (4) to allow the user to designate the signs in the first series (3) which constitute said confidential information; and

- means for validation of the entries.

12. Terminal according to claim 11, characterized in that it includes a keyboard (1) which is distinct from the display means and which is equipped with a plurality of keys (5), each of these keys on the keyboard being identified by a sign which belongs to said second series of signs (4), and in that pressing each key on said keyboard whose sign corresponds to the sign in the second series (4) displayed opposite one of the signs constituting said

confidential information corresponds to the entry of this sign constituting said confidential information.

13. Terminal according to claim 11, characterized in that it comprises:

- means for memorizing at least one reference sign that is known to the user and belongs to the second series of signs (4); and

- means which permit the user to display the signs in the first series (3) in such a way that the signs constituting the confidential information are disposed opposite said reference sign.

14. Terminal according to claim 11, characterized in that the second series of signs (4) includes a number of distinct signs that is less than the number of signs in the first series (3).

15. Terminal according to claim 11, characterized in that the signs in the second series (4) are different from those in the first series (3).

THIS SHEET HAS BEEN REPLACED

A B R E G E

Inventors: Jacques Patarin, Michel Ugon

With the confidential information being composed of signs which belong to a first series (3), a second series of signs (4) is defined, the first and second series of signs are displayed in a relatively random position, and this placement in correspondence is used to enter the confidential information in such a way that a third party who observes the entry operations cannot determine the confidential information.

The invention also relates to the terminal associated with this process.

Fig. 1.

This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

This Sheet Has Been Replaced

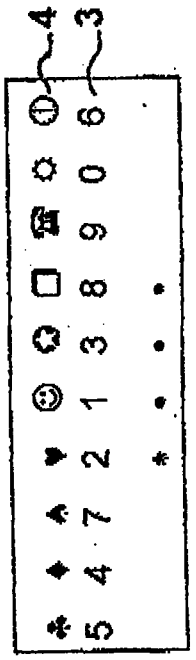

FIG. 2

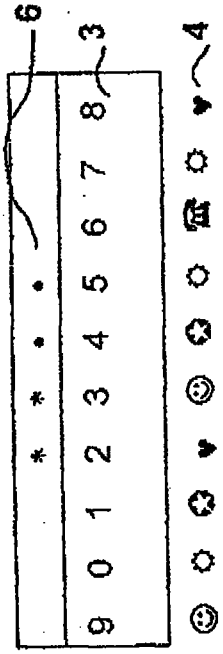

FIG. 3

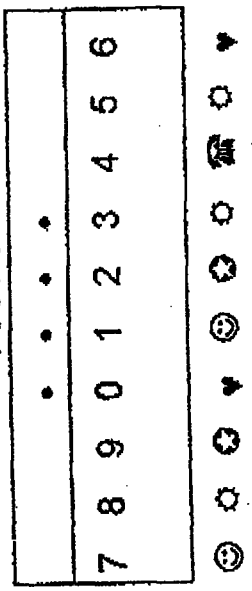

FIG. 4

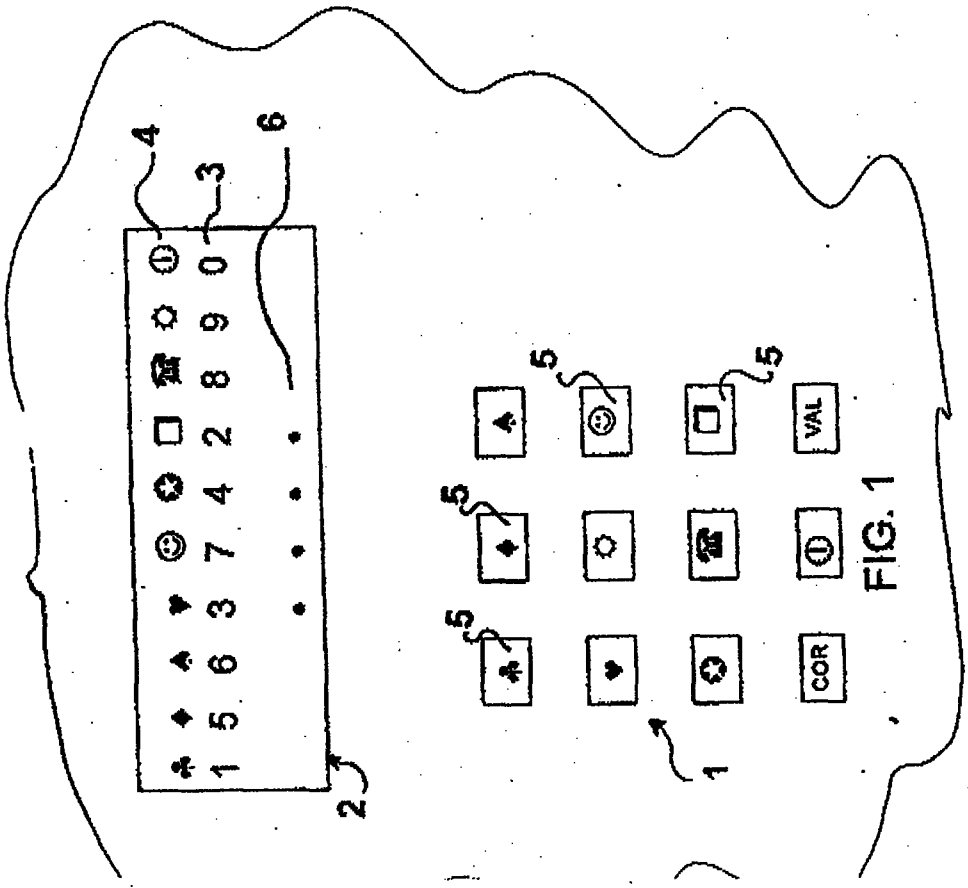

FIG. 1

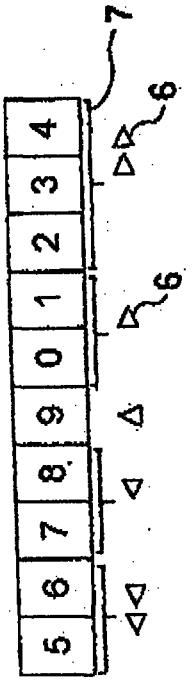

FIG. 5

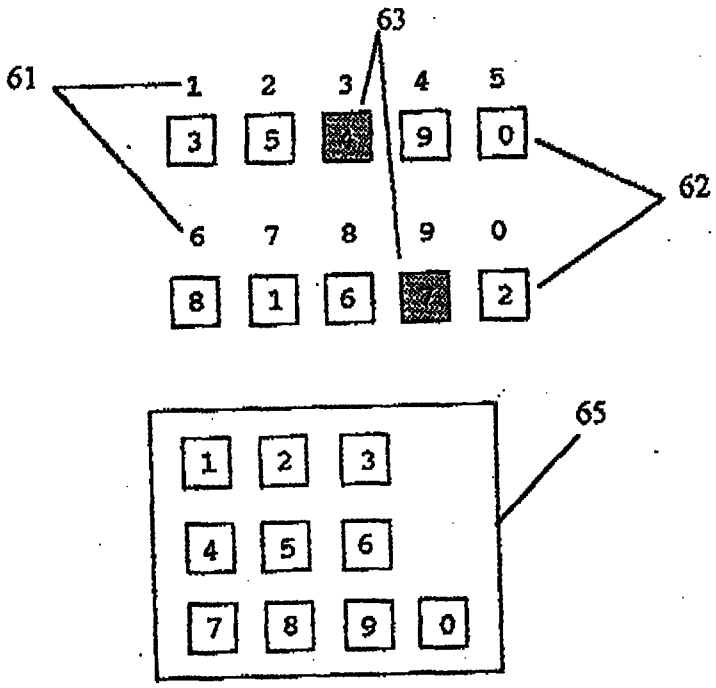

FIG. 6

9606083-5

IPO8'
COPY #21

REPLACEMENT SHEET
02 JUN 1997

ABSTRACT

PROCESS FOR ENTRY OF A CONFIDENTIAL PIECE
OF INFORMATION AND ASSOCIATED TERMINAL

With the confidential information being composed of signs which belong to a first series (3), a second series of signs (4) is defined, the first and second series of signs are displayed in a relatively random position, and this placement in correspondence is used to enter the confidential information in such a way that a third party who observes the entry operations cannot determine the confidential information.

The invention also relates to the terminal associated with this process.

Fig. 1.

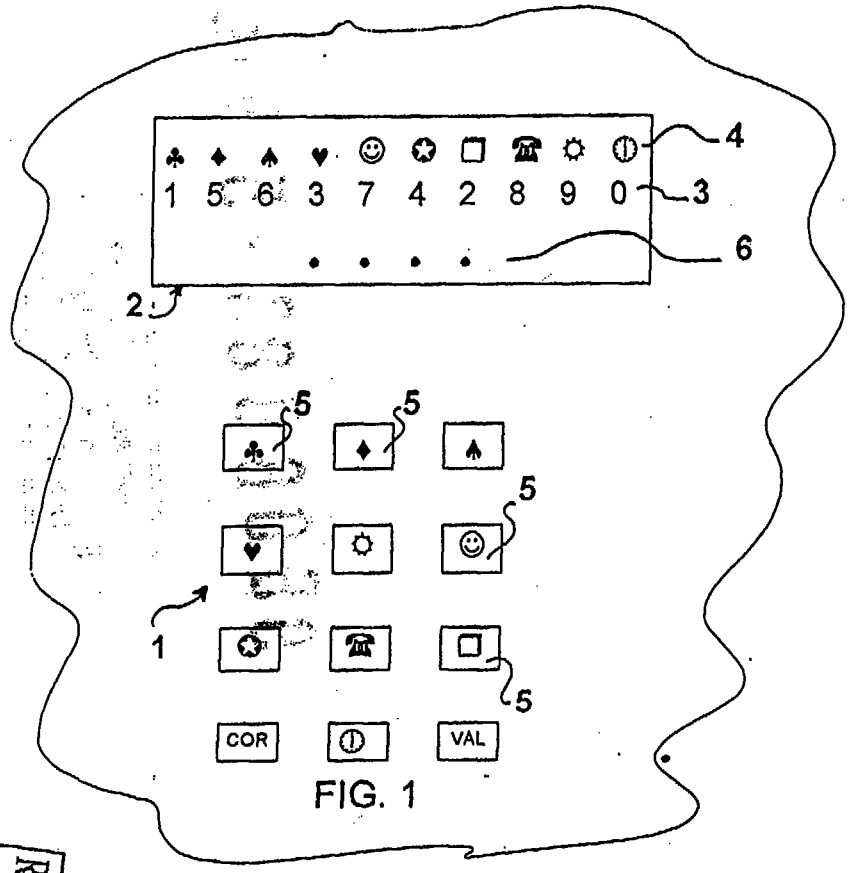

FIG. 1

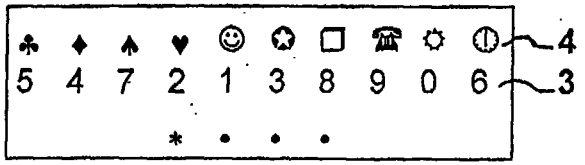

FIG. 2

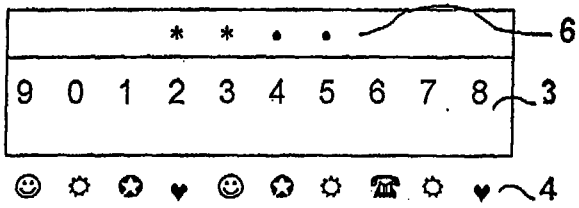

FIG. 3

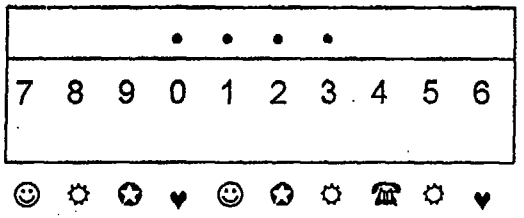

FIG. 4

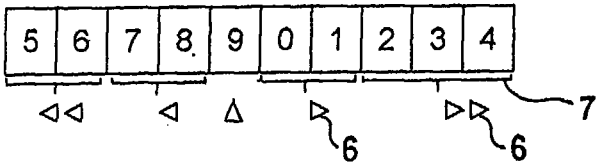

FIG. 5

REPLACEMENT SHEET
02 JUN 1997

#3

REPLACEMENT SHEET
13 AUG 1999

* C L M S *

first series (3).

11. Terminal comprising display means and means to enter a confidential piece of information furnished by a user, said information including a plurality of signs which belong to a first set of signs (3), said terminal being characterized in that it is arranged so as to display said first and a second series of signs (4) in such a way that each sign in the first series (3) is disposed opposite a sign in the second series (4), and it includes:

- means for using the signs in the second series (4) to allow the user to designate the signs in the first series (3) which constitute said confidential information.

12. Terminal according to claim 11, characterized in that it includes a keyboard (1) which is distinct from the display means and which is equipped with a plurality of keys (5), each of these keys on the keyboard being identified by a sign which belongs to said second series of signs (4), and in that pressing each key on said keyboard whose sign corresponds to the sign in the second series (4) displayed opposite one of the signs constituting said confidential information corresponds to the entry of this sign

REPLACEMENT SHEET

11 JAN 2002

4. In this figure, a new shift has been executed between the series of digits forming the first series of signs and the second series of signs. It so happens that the choice between the 1 and the 4 which could have been noted by an observer during the preceding entry, is now illustrated by a ☺ and a ☎, which means that there is one chance in two that the defrauder will make a mistake in the entry of the first sign constituting the confidential information. Likewise, a defrauder will again have a doubt concerning the second sign to be entered, since the digits 0, 5 and 7 which corresponded to the sign ✡ in Fig. 3 are represented in Fig. 4 by the signs ♥, ✡ or ☺. Note that the probability of an observer's being able to reenter the confidential information exactly is extremely low. This risk is further minimized if, as previously, it has been arranged for the correspondence between the first series of signs and the second series of signs to change each time a sign has been entered.

The variant in Fig. 5 is distinguished from that in Fig. 3 in that the sophisticated icons constituted by the signs in the second series have been replaced here by simpler signs which are made from a single elementary sign, namely an isosceles triangle. The second series of signs comprises five signs, each of which is distinguished by a specific number of triangles or by a specific orientation of them. Thus, all three of the digits 2 through 4 in the first series of signs are designated by the same sign,